Speakers: Threat Hunting Team at Morgan Stanley

Bro in the Financial Services Sector: Developing a strategy for Threat Hunting

Hunting for cyber intrusions in a financial services environment offers some interesting technical and business challenges from complex networks to regulatory oversight. In this presentation, we will focus on Bro's Protocol Identification and Validation process and other techniques that can be used to model data sets for effective threat hunting in a complex network without causing business impact.
Understanding the business. It is important to understand how and why various protocols were introduced to the environment to identify malicious activity.

Inventory the protocols. Every market, product, and data feed are a little different and, in many instances, the protocols are used in vastly different ways than their technical designed purpose. While some abide by industry best practices others were developed before there were standards or to support a specific need and continue to be used in day-to-day business operations.

Categorize protocols. There are two primary buckets for the purposes of threat hunting: known versus unknown. Once placed in these buckets, they can be analyzed for malicious activity and routed to the appropriate response team for remediation.

Continuous improvement. Continuing to refine analytics, tune protocol analyzers and keep abreast of the latest capabilities will enable earlier detection.